ORIGINAL

BEFORE THE

Federal Communications Commission

WASHINGTON, DC 20554

In the Matter of	)	
	)	
Communications Assistance	)	CC Docket No. 97-213
for Law Enforcement Act	)	

COMMENTS OF AIRTOUCH COMMUNICATIONS, INC.

AIRTOUCH COMMUNICATIONS, INC.

AirTouch Communications, Inc.
1818 N Street, N.W.
Suite 800
Washington, D.C. 20036
(202) 293-3800

Michael W. Mowery
AirTouch Communications, Inc.
2999 Oak Road, MS1025
Walnut Creek, CA 95596
(510) 210-3804

Attorneys for AirTouch Communications, Inc.

May 20, 1998

Table of Contents

Page

Summary

The Federal Bureau of Investigation and Department of Justice (collectively, "FBI") have petitioned the Commission to rule that the industry standard implementing CALEA's assistance capability requirements is incomplete and deficient under the Communications Assistance for Law Enforcement Act ("CALEA"). AirTouch demonstrates herein that the Commission must reject the Petition in its entirety because none of the additional capabilities the FBI seeks meets the statutory standards Congress established in CALEA.

Congress directed the Commission to "narrowly interpret" CALEA's obligations, noting that CALEA was designed "to *preserve* the government's ability . . . to intercept communications involving advanced technologies" and that CALEA's assistance capability requirements constitute "both a floor and a ceiling." In this regard, the FBI Director assured Congress that CALEA would "preserve the status quo" and "provide law enforcement no more and no less access to information than it had in the past." The FBI now wants the Commission to disregard these clear mandates by requiring a whole set of new features designed to *expand,* rather than "preserve," law enforcement interception capabilities — including new features even the FBI concedes are not mandated by the statute.

AirTouch's comments analyze each of the "punch list" items raised by the FBI. Some of the items are not required by CALEA. Others are flatly inconsistent with CALEA and raise significant privacy issues. Still other items need not be provided because they do not meet other statutory criteria, including the requirements that the capability be "reasonably available to carriers" or can be deployed by "cost-effective methods."

Moreover, completely inconsistent with CALEA is the FBI's request that the Commission require carriers to implement the industry standard as the *Commission* may modify. Congress made clear that "[t]he legislation leaves it to each carrier to decide how to comply. . . . Compliance with the industry standards is voluntary, not compulsory. *Carriers can adopt other solutions for complying with the capability requirements.*" Thus, while the Commission has the authority to determine what capabilities CALEA requires and prohibits, it does not have the discretion to mandate to industry how to implement those capabilities. The Commission cannot remove by regulation the very flexibility Congress decided by statute that carriers should enjoy. If law enforcement believes that a particular carrier's practices are unreasonable, it can invoke the procedure established in CALEA: seek an enforcement order.

The current industry standard meets (and may well exceed) CALEA's requirements. Commission affirmation of this standard would enable industry to implement CALEA most quickly — because vendors would not require additional time to develop punch list capabilities and then change their completed work implementing the industry standard to incorporate new modifications. If, however, the Commission determines that the industry standard is deficient, it should remand the task of developing implementing technical standards to TR-45.2, the TIA subcommittee which adopted the industry standard under review. This subcommittee is equipped to ensure that any modifications which the Commission may order are consistent with all existing standards and protocols, including the new Lawfully Authorized Electronic Surveillance protocol which TR-45.2 developed specifically to implement CALEA.

Finally, CALEA requires the Commission to establish a new compliance date now that the industry standard has been challenged. A new compliance date cannot realistically be set without first knowing the results of the Commission's decision, which will determine what additional capabilities, if any, must be included within the standard. Consequently, assuming the Commission in the interim grants the pending requests to extend the current October 1998 compliance deadline, AirTouch recommends that the Commission seek additional comment regarding a new compliance deadline after the order is released, so industry can submit realistic and specific proposals based on the Commission's order.

BEFORE THE

Federal Communications Commission

WASHINGTON, DC 20554

In the Matter of	)	
	)	
Communications Assistance	)	CC Docket No. 97-213
for Law Enforcement Act	)	

COMMENTS OF AIRTOUCH COMMUNICATIONS, INC.

AirTouch Communications, Inc. ("AirTouch") submits these comments in opposition to the Joint Petition for Expedited Rulemaking filed by the Federal Bureau of Investigation and the U.S. Department of Justice ("FBI Petition").[1] As demonstrated below, none of the additional capabilities the FBI wants the Commission to impose on carriers meet the statutory standard Congress has established in the Communications Assistance for Law Enforcement Act ("CALEA"); the Commission should, therefore, reject the FBI Petition in its entirety.

I. Introduction and Background

Congress has determined that the Commission should play a central role in CALEA's implementation. Among other things, the Commission has been charged with determining *what* specific assistance capabilities industry should and should not provide to law enforcement,[2] and *when* industry should begin making these capabilities available.[3] The

---

1 *See Public Notice*, CC Docket No. 97-213 "Communications Assistance for Law Enforcement Act," DA 98-762 (April 20, 1998).

2 *See* 47 U.S.C. § 1006(b); *see also* H.R. Rep. No. 103-827, at 27 (1994) ("House Report") ("The FCC retains control over the standards.").

3 *See* 47 U.S.C. §§ 1006(b)(5); 1006(c); *see also* House Report at 27 ("[T]he FCC is required to . . . establish a reasonable time and conditions for compliance with and the

(continued...)

Commission's role is critical because it is through the Commission that Congress intended "to balance three key policies":

> (1) to preserve a narrowly focused capability for law enforcement agencies to carry out properly authorized intercepts; (2) to protect privacy in the face of increasingly powerful and personally revealing technologies; and (3) to avoid impeding the development of new communications services and technologies.[4]

Moreover, Congress decided that "public accountability" was to be a hallmark of CALEA implementation, stating that "*all* proceedings before the FCC will be subject to public scrutiny, as well as congressional oversight and judicial review."[5]

Congress enacted CALEA in October 1994, and it encouraged industry to develop implementing technical standards "[t]o ensure the efficient and industry-wide implementation of the assistance capability requirements. . . ."[6] Industry completed a substantial first draft within a year (by late 1995), but unanticipated delays (involving the FBI) postponed the publication of the standard until December 1997.[7] The U.S. Department of Justice and Federal Bureau of

---

3 (...continued)
transition to any new standard."); at 28 ("The FCC may grant a petition for relief from compliance with the assistance capability requirements.").

4 House Report at 13.

5 *Id.* at 14, 20 (emphasis added); *see also id.* at 27-28.

6 *See* 47 U.S.C. § 1006(a)(1). The incentive Congress established was to give carriers a "safe harbor" to the extent they deployed equipment compliant with the publicly-available industry standard. *See id.* § 1006(a)(2). Only after it was too late for manufacturers to develop capabilities based upon the industry standard by the statutory deadline did the FBI finally acknowledge that the industry standard meets this "safe harbor" provision. *See* FBI Comments, CC Docket No. 97-213, at 6 ¶ 8 (May 8, 1998).

7 Industry initially postponed ballot of the draft standard at the FBI's request, although subsequent, extended discussions with the FBI were unsuccessful. Thereafter, at the FBI's recommendation, law enforcement twice vetoed the industry standard — not

(continued...)

Investigation (collectively, "FBI") have petitioned the Commission to rule that the industry standard is incomplete because it does not include additional capabilities which they deem important.[8] At the other end, the Center for Democracy and Technology ("CDT") has petitioned the Commission to rule that, not only is the FBI's petition contrary to CALEA, but that two capabilities in the industry standard — location tracking and packet data — are prohibited by CALEA as well.[9]

Congress has established the standard the Commission should utilize in evaluating these two "deficiency petitions" and has directed the Commission to "narrowly interpret" CALEA's requirements, as AirTouch points out in Section II. The Commission's task in ruling on these deficiency petitions, however, is made more arduous for several reasons noted below.

A. The FBI's "Punch List" as a Moving Target. Industry continues to have difficulty understanding the precise features which the FBI is demanding.[10] Part of the problem is that the FBI changes its position. For example, in its March 27, 1998 Petition, the FBI

---

7 (...continued)
because it was troubled by the adequacy of the standard itself, but rather because it believed the standard was incomplete because it did not include the FBI's additional "punch list" capabilities.

8 *See* FBI/DOJ, Joint Petition for Expedited Rulemaking, CC Docket No. 97-213 (March 27, 1998) ("FBI Petition").

9 *See* CDT, Petition for Rulemaking Under Sections 107 and 109 of CALEA, CC Docket No. 97-213 (March 26, 1998) ("CDT Petition").

10 Indeed, there is even uncertainty over the number of punch list items the FBI seeks to impose on industry. Most of the industry believes the FBI is seeking nine items, based on the DOJ letter declaring that two of the FBI's items were not required by CALEA. *See* Letter from Stephen R. Colgate, Assistance Attorney General for Administration, to Tom Barba, Steptoe & Johnston (Feb. 3, 1998). However, in its petition, it appears that the FBI is asking the Commission to impose 10 of its original punch list items, including item 8 (standardized delivery interfaces) which the DOJ determined was not required by CALEA. *Id.*

requests the delivery of certain "call event messages . . . no later than three seconds after the occurrence of the associated call event."[11] However, in a proposal to industry submitted only two weeks earlier, the FBI demanded that "[c]all event messages shall be delivered . . . within 500 milliseconds."[12] Similarly, the FBI's Petition asks that the Commission limit delivery interfaces to five,[13] when weeks earlier the FBI appeared to agree with industry that such a limitation was impractical and undesirable. In addition, the FBI still has been unable to provide industry a description of its "punch list" capabilities sufficient to enable industry to begin developing technical standards implementing the list — and the FBI's delays, in turn, have delayed industry's effort to define the punch list in a manner which industry can understand and implement.[14]

B. Difficulty in Acquiring Relevant Cost Data. CALEA deployment costs are a critical component of the Commission's statutory inquiry, as AirTouch explains in Section II below. For example, CALEA directs the Commission to "minimize" the cost of CALEA compliance on residential consumers, and specifies that a disputed capability may be imposed on

---

11 *See* FBI Proposed Rule 64.1708(e)(3).

12 *See* FBI Contribution, TR.43.2.ESS/98.03.10.3, at 13 (March 10, 1998).

13 *See* FBI Petition at 57-58 ¶¶ 104-05.

14 To confirm, industry believes the FBI's punch list items are not required by, and are inconsistent with, CALEA. Nevertheless, in an effort to cooperate and keep the process moving, industry, under the auspices of TR-45.2, has formed an Enhanced Surveillance Services ("ESS") *ad hoc* group attempting to develop technical standards concerning the "punch list." The ESS group has been meeting monthly since the beginning of the year. AirTouch understands that sometimes FBI personnel attend; sometimes they do not. The ESS group has recently had to defer the target dates for its workplan because the FBI has still not submitted its preferred requirements in sufficient detail.

carriers only if it can be deployed "by cost-effective methods."[15] While vendors have calculated their estimated costs to develop the challenged punch list capabilities and have recently submitted this data to the FBI,[16] this data is necessarily preliminary and AirTouch has had difficulty acquiring this data from some of its vendors.[17] While the data is preliminary only, it appears that the costs to develop the punch list capabilities will be enormous.

Carriers who may be asked to pay for challenged capabilities need to know this information and it should be part of the public record in this proceeding; indeed, the Commission requires cost data to discharge its statutory responsibility. The Commission should therefore direct the FBI to disclose this estimated cost data (1) so carriers and the public have some indication of the likely cost impact of each of the FBI's "punch list" items, and (2) so the Commission can analyze cost factors in rendering its decision, as CALEA requires.[18]

C. Apparent Attempts to Undermine the Commission's Authority. AirTouch is concerned about recent FBI activity which has the potential effect of undermining the decision-making authority Congress expressly placed in the Commission alone. For example, the FBI

---

15 47 U.S.C. § 1006(b)(1) and (3).

16 The FBI's statement in its petition that "cost information . . . is in the possession of industry rather than law enforcement," while perhaps accurate at the time made, is no longer accurate today. *See* Petition at 62 ¶ 111. Moreover, as discussed herein, carriers have, for the most part, *not* been given specific costing data from vendors.

17 For example, one vendor advised AirTouch that it "[r]ecently . . . provided pricing estimates to the Department of Justice. However, those estimates were based upon numerous assumptions and conditions to which the Department of Justice has not yet agreed. Thus, it is impossible to provide you with accurate pricing information at this time."

18 While vendors also have access to this data, vendors have understandable proprietary and business concerns about public disclosure of sensitive data. To address this concern, the FBI should submit this data for the record because it can list specific costing information without revealing the names of the affected vendors.

wants vendors to enter into "enforcement forbearance agreements" to determine what capabilities their equipment will provide and when.[19] It is AirTouch's understanding that the FBI is pressing vendors to agree "voluntarily" to develop its "punch list" capabilities — even though the statute imposes on the *Commission* the responsibility to determine the lawfulness of these challenged features to ensure that privacy and cost factors are given adequate consideration and to ensure "public accountability." Moreover, AirTouch finds especially troubling the FBI's recent suggestion that carriers are free to *ignore* the Commission's orders in this proceeding by providing capabilities which the Commission may determine are inconsistent with CALEA.[20]

D. Law Enforcement Interceptions Will Continue During This Proceeding.

Contrary to law enforcement suggestions, it is important to emphasize that the Commission's consideration of, and decision regarding, the FBI Petition will *not* impact law enforcement's ability to continue to conduct "basic" interceptions. Since the inception of the broadband CMRS industry over a decade ago, AirTouch and other CMRS providers have assisted law enforcement to meet its interception requirements. Indeed, last year law enforcement conducted a record number of interceptions — without CALEA having been implemented.[21] During the pendency of this proceeding, AirTouch and other carriers will continue to assist law enforcement in its conduct of authorized interceptions.

---

19 *See, e.g.*, FBI Comments at 17-19 ¶¶ 31-33 (May 8, 1998).

20 *See* FBI Comments at 16 ¶ 30 (May 8, 1998) ("The carrier will not be *required* to remove these capabilities" which the Commission determines are inconsistent with CALEA) (emphasis in original).

21 During 1997, federal and state judges approved a total of 1,186 wiretap requests, and federal and state law enforcement agencies conducted a total of 1,094 taps. *See* Administrative Office of the U.S. Courts, 1997 Wiretap Report (April 1998). Of these wiretaps, only 206 were conducted on cellular, paging, and e-mail accounts. *Id.*

II. Congress Has Directed The Commission To "Narrowly Interpret" CALEA's Assistance Capability Requirements

Congress has charged the Commission alone with resolving law enforcement's contention that the industry standard implementing CALEA's assistance capability requirements is deficient.[22] It has also established the legal standard the Commission is to apply in reviewing a deficiency petition. Specifically, "if a Government agency or any other person believes that such . . . [industry] standards are deficient, the agency or person may petition the Commission to establish, by rule, technical requirements or standards that" —

> (1) meet the assistance capability requirements of section 103 by cost-effective methods;
>
> (2) protect the privacy and security of communications not authorized to be intercepted;
>
> (3) minimize the cost of such compliance on residential ratepayers; [and]
>
> (4) serve the policy of the United States to encourage the provision of new technologies and services to the public.[23]

Congress further made clear that in applying this four-part standard, the Commission should "narrowly interpret" CALEA's assistance capability requirements:

> The Committee intends the assistance requirements in section [103] to be both a floor and a ceiling. . . . The Committee urges against overbroad interpretation of the requirements. . . . The

---

22 *See* 47 U.S.C. § 1006(b); *see also* House Report at 27 ("The FCC retains control over the standards. . . . [CALEA] provides a forum at the Federal Communications Commission in the event a dispute arises over the technical requirements or standards.").

23 47 U.S.C. § 1006(b)(1)-(4). In addition, as discussed in Part VI *infra,* Congress directed the Commission to "provide a reasonable time and conditions for compliance with and the transition to any new standard, including defining the obligations of telecommunications carriers under section 103 during any transition period." *Id.* § 1006(b)(5).

> Committee expects industry, law enforcement and the FCC to narrowly interpret the requirements.[24]

In this regard, the FBI Director assured Congress that CALEA would "preserve the status quo" and "provide law enforcement no more and no less access to information than it had in the past."[25]

As AirTouch demonstrates herein, the FBI wants the Commission to disregard the Congressional directive to "narrowly interpret" CALEA's requirements by imposing a whole set of new features designed to *expand,* rather than "preserve," law enforcement interception capabilities — including new features the FBI concedes are not mandated by the statute.

III. The FBI Has Failed to Meet Its Burden to Demonstrate that the Additional Capabilities It Seeks Are Consistent With CALEA

In its Petition, the FBI asks the Commission to order carriers to deploy 10 of its original "punch list" capabilities, plus another capability not previously included in its punch list.[26] AirTouch demonstrates below that the FBI has failed to meet its burden that these additional capabilities are consistent with CALEA.

One general observation is appropriate at the outset. As noted above, in evaluating the FBI's Petition the Commission is "to encourage the provision of new technologies and services to the public" and to "minimize" CALEA compliance costs on residential

---

24 House Report at 22-23; *see also id.* at 13, *quoted* on page 2 *supra.*

25 *Id.* at 22; *see also* FBI Petition at 19 ¶ 32 ("CALEA thus does not expand law enforcement agencies' power or authority to conduct electronic surveillance; that authority continues to be defined principally by Title III.").

26 The FBI appears to have abandoned its request for punch list item 11, separated delivery. In these comments, AirTouch refers to the punch list as documented in Attachment A to the letter from Stephen R. Colgate, Assistant Attorney General for Administration, to Tom Barba, Steptoe & Johnson (Feb. 3, 1998). AirTouch follows the organization used by the FBI in its Petition.

consumers.[27] The FBI asserts that its proposed punch list will "not impose any material restrictions on the adoption and the provision of new technologies and services to the public" and will impose "the least financial burden on residential ratepayers."[28]

AirTouch cannot agree with the FBI's unsupported assertions. Vendors have advised AirTouch that, in developing solutions which comply with the industry standard, they have already diverted resources from other projects which would provide new features and services to the public. Moreover, these vendors have told AirTouch that they will be required to divert significantly more resources if they are required to implement the punch list. In fact, one vendor has advised AirTouch that the development of modifications incorporating the punch list alone could require *additional effort over 160% above* the substantial effort required to meet the industry standard. It is thus apparent that implementation of the punch list would be costly and likely rate impacting, and would divert finite vendor resources from developing new technologies and services that the public demands.

A. A New, Expanded Conference Call Capability (Punch List Item 1)

Consistent with past practice, the industry standard would permit law enforcement to intercept a conference call as long as the subject of a court order, or another person using the subject's phone, remains connected to the call.[29] Although CALEA was designed to "*preserve*

---

27 47 U.S.C. § 1006(b)(3) and (4).

28 FBI Petition at 62 ¶ 111 and 63 ¶ 113. In this regard, there obviously could be no factual basis for the FBI's opinion that its punch list would have minimal cost impact on residential consumers, given that, as the FBI acknowledges, at the time it filed its Petition it did not have access to cost data (although it obtained vendor information since then). *See* FBI Petition at 62 ¶ 111.

29 Even the FBI acknowledges that the industry standard "does not amount to a reduction in the information that has been available to law enforcement under POTS." FBI Petition at

(continued...)

the government's ability . . . to intercept communications,"[30] and although the FBI Director testified that CALEA would provide law enforcement with "no more and no less access to information than it had in the past,"[31] the FBI now contends that the industry standard is "plainly deficient" because it does not include a new capability never before made available to law enforcement.[32] According to the FBI, carriers should also be required to allow law enforcement to intercept conference calls even "*after the subject leaves the conversation.*"[33] In essence, the FBI wants the Commission give law enforcement the right to intercept, *without any additional court order*, the communications of persons when the subject of the existing court order does not even participate in the call.[34]

There are numerous problems with this proposal — in addition to the fact that the FBI wants industry to provide a *new* capability as opposed to "preserving" an existing

---

29 (...continued)
30 ¶ 51.

30 House Report at 9 (emphasis added); *see also id.* at 16 ("The legislation requires telecommunications common carriers to ensure that new technologies and services *do not hinder* law enforcement access to the communications of a subscriber who is the subject of a court order authorizing electronic surveillance. The bill *will preserve* the government's ability . . . to intercept communications that utilize advanced technologies.") (emphasis added).

31 *Id.* at 22.

32 FBI Petition at 32 ¶ 55.

33 FBI Proposed Rule 64.1708(a) (emphasis added).

34 The FBI wants the Commission to expand the scope of its interception authority because the lack of this new communications "*could deprive* investigators and prosecutors of important evidence." FBI Petition at 31 ¶ 53 (emphasis added). The FBI is making its arguments to the wrong forum. If the FBI believes the expanded interception capabilities it desires could be important, it should present its arguments to Congress.

capability.[35] At the outset, there is a substantial question whether law enforcement is authorized to intercept the requested communications without the receipt of an additional court order identifying one or more participants on the call.[36] The nation's interception laws were designed "to protect effectively the privacy of wire and oral communications."[37] Congress has declared:

> To safeguard the privacy of innocent persons, the interception of wire or oral communications where none of the parties to the communications has consented to the interception should be allowed only when authorized by a court of competent jurisdiction and should remain under the control and supervision of the authorizing court.[38]

---

35 In addition, the FBI's Proposed Rule 64.1708(a)(1), specifying the number of call content delivery channels required to implement this feature, appears to involve a *capacity* requirement beyond the scope of this proceeding, which is limited to the *capabilities* which CALEA requires.

36 Congress included the subject identification requirement to "reflect . . . the constitutional command of particularization." S. Rep. No. 90-1097, at 101 (1968); *see also United States v. Donovan,* 429 U.S. 413, 428 (1977) ("We therefore conclude that a wiretap application must name an individual if the Government has probable cause to believe that the individual is engaged in the criminal activity under investigation and expects to intercept the individual's conversations over the target telephone.").

37 Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. 90-351, Title III § 801(b), 82 Stat. 211 ("Title III"). Congress enacted Title III because the Supreme Court had held that law enforcement's prior interception practices were unconstitutional. *See, e.g., Katz v. United States*, 389 U.S. 347 (1967); *Berger v. New York*, 388 U.S. 41 (1967).

38 Title III § 802(d), 82 Stat. 211.

Thus, law enforcement may intercept a communications only upon receipt of a court order[39] — an order that must "identify the person, if known, whose communications are to be intercepted" and "the place where authority to intercept is to be intercepted."[40]

With its expanded conference call capability, the FBI seeks authority to intercept communications when the subject of the court order does not participate in the call. On its face this FBI request would appear to be inconsistent with the prohibition on the interception of communications without a court order.[41]

Further, CALEA directs the Commission, in evaluating a proposed capability, "to protect the privacy and security of communications not authorized to be intercepted."[42]

> In taking any action under this [deficiency petition] section, the FCC is directed to protect the privacy and security of communications *that are not the targets of court-ordered electronic surveillance* . . . .[43]

---

39 Under certain limited "emergency situations," law enforcement may commence interceptions without a court order so long as an application for such an order is made within 48 hours. *See* 18 U.S.C. § 2518(7).

40 18 U.S.C. §§ 2518(1)(b) and (4)(a) and (b). As the FBI points out, once armed with a court order, it may also intercept communications involving other persons using the subject's telephone. *See* Petition at 28-29 ¶¶ 48-49. In these circumstances, law enforcement is obligated to "minimize the interception of communications not otherwise subject to interception." 18 U.S.C. § 2518(5). However, in this case the FBI wants to intercept private communications *after law enforcement learns that the subject of the court order has left the call.* Given the statutory minimization requirement, there would appear no legal basis for law enforcement to intercept the conference calls in question without obtaining a separate court order identifying one of the remaining conference call participants.

41 *See* 18 U.S.C. § 2511.

42 47 U.S.C. § 1006(b)(2).

43 House Report at 27 (emphasis added).

CALEA also imposes this same affirmative obligation directly on carriers.[44] With its expanded conference call capability, the FBI effectively seeks the right to intercept, *without a court order,* communications of persons which "are not the targets of court-ordered electronic surveillance." In AirTouch's judgment, the FBI request raises serious issues of privacy under the Fourth and Fifth Amendments to the U.S. Constitution and under interception laws.

There are problems with the FBI proposal aside from these privacy concerns. CALEA states that the Commission may impose a capability on carriers only if it "meet[s] the assistance capability requirements of section 103 *by cost-effective methods.*"[45] Thus, by statute the Commission must engage in a cost-benefits analysis to determine whether the value of the capability in question outweighs the costs carriers would incur in deploying the capability.[46]

AirTouch's preliminary discussions with vendors indicate that this requested capability could be expensive to deploy, but as discussed above, AirTouch has been unable to obtain from all its vendors their estimated cost data to develop this feature. The Commission should require the FBI to make this cost data available for public comment (without naming vendors individually), so the Commission, consistent with its statutory directive, can make an

---

44 *See* 47 U.S.C. § 1002(a)(4)(A).

45 *Id.* § 1006(b)(1) (emphasis added).

46 That Congress intended the Commission to engaged in a cost-benefits analysis is further confirmed by the directive that the capability in question "minimize the cost of such compliance" on residential consumers. 47 U.S.C. § 1006(b)(3); *see also* House Report at 28 (defining the 'reasonably achievable' standard as a "limitation . . . intended to excuse a failure to comply with the assistance capability requirements . . . where the total cost of compliance is wholly out of proportion to the usefulness of achieving compliance for a particular type of category of services or features."). There is, therefore, no basis to the FBI's argument that carriers must provide any new capability so long as "industry has not identified [a] less expensive means" of providing the same capability. FBI Petition at 59-60 ¶ 108.

independent determination whether this capability (assuming *arguendo* it is encompassed within CALEA) can be deployed "by cost-effective methods."

However, there is a substantial question whether the proposed expanded conference call feature can be justified under any cost-benefits analysis — because it would appear to be easy for criminals to bypass this feature if carriers were to deploy it. The FBI's proposal would enable law enforcement to intercept *only* those conference calls which are established by the subject of the court order (or another person using the subject's phone) *and* which are supported by a conference service provided by the subject's serving local carrier. Under the FBI's proposal, law enforcement would *not* be able to intercept conference calls when the subject no longer participates if either (a) the call is set-up by another person using another telephone, or (b) the subject initiates the call but uses a conference bridge service offered by another carrier or service provider. Given the ease in which criminals could bypass the FBI's proposed feature, AirTouch submits that this is an additional reason why carriers should not be required to expend capital and effort to deploy this new capability.

B. Additional Call-Identifying Information (Punch List Items 2, 3, 4, and 10)

CALEA obligates carriers to enable law enforcement "to access call-identifying information that is reasonably available to the carrier."[47] The FBI acknowledges that the industry standard provides for "most call-identifying information associated with the initiation and completion of a call."[48] However, it contends that the standard omits four "vital" capabilities that

---

47 47 U.S.C. § 1002(a)(2).

48 FBI Petition at 35 ¶ 60.

render the standard "fundamentally deficient."[49] Specifically, the FBI asks the Commission to order carriers to provide the following four additional "punch list" capabilities:

1. Flash Hook/Feature Keys (Punch List Item 3). The FBI wants to receive a data message when the subject of a court order presses a feature key or flash hook to hold or transfer a call.[50]

2. Post-Cut-Through Dialing (Punch List Item 10). The FBI wants a CMRS provider to provide any digits the subject may press after the CMRS provider completes set-up of its portion of the call.[51]

3. Information on Participants in a Multi-Party Call (Punch List Item 2). The FBI wants carriers to deliver certain new data messages, such as a "party hold" message, to advise law enforcement about which parties are participating on a conference call.[52]

4. Access to Network-Generated Signaling (Punch List Item 4). The FBI wants carriers to deliver certain network signals such as ringing and a busy signal.[53]

---

49 *Id.* at 35 ¶ 60 and 38 ¶ 65. Although the FBI actually states that the industry standard omits "three vital capabilities," id., its section discussing "subject-initiated dialing" includes two different punch list items — flash hook/key features (No. 3) and post-cut-through dialing (No, 11) — and the FBI proposes the adoption of two different rules. *Compare* note 55 with note 56 *infra.*

50 *See* FBI Petition at 36-38 ¶¶ 61-65; Proposed Rule 64.1708(c).

51 *See* FBI Petition at 39-42 ¶¶ 68-72; Proposed Rule 64.1708(i).

52 *See* FBI Petition at 42-45 ¶¶ 73-79; Proposed Rule 64.1708(b). This request is related to the enhanced conference call feature in punch list item 1. It thus suffers from the same flaw as punch list item 1 (*e.g.*, the ease by which the feature may be bypassed by using an unaffiliated conference bridge service).

53 *See* FBI Petition at 45-47 ¶¶ 80-82; Proposed Rule 64.1708(d).

In addition, in what appears to be a new request not previously contained in its punch list, the FBI also asks that all call-identifying information be delivered to law enforcement over a call data channel (as opposed to some information being delivered over a call content channel).[54]

Many of the additional capabilities the FBI seeks are outside the scope of CALEA because they do not fall within the statutory definition of call-identifying information. CALEA defines call-identifying information to mean information "identifying" a call — that is, "dialing or signaling information that identifies the *origin, direction, destination, or termination* of each communication generated or received by a subscriber."[55] Some of the capabilities the FBI requests, including signals that a party has been placed "on hold" or network signals indicating ringing or a busy signal, do not involve "the origin, direction, destination, or termination" of a call. As a result, these capabilities do not fall within the statutory definition of "call-identifying information," and carriers would therefore contravene CALEA if they provided this information to law enforcement. It bears repeating that Congress clearly stated that the assistance capabilities it specified are "both a floor and ceiling."[56]

Other capabilities which the FBI seeks may in fact fall within the statute's definition of call-identifying information.[57] For example, certain (but not all) post-cut-through

---

54 *See* FBI Petition at 47-49 ¶¶ 83-85; Proposed Rule 64.1708(d) and (i)(1).

55 47 U.S.C. § 1001(2) (emphasis added). The limited scope of the call-identifying information definition is further confirmed by CALEA's legislative history. *See* House Report at 21 ("The term . . . means the dialing or signaling information generated that identifies the origin and destination of a wire or electronic communication.").

56 *See* House Report at 22.

57 A good example involves so-called "post-cut-through" digits, which may be dialed to control CPE or to direct the destination of a call. The latter would appear to be encompassed within the statutory definition of call-identifying information; the former would

(continued...)

digits may identify "the origin, direction, destination, or termination" of a call.[58] However, CALEA is clear in specifying that carriers need deliver to law enforcement only "call-identifying information that is *reasonably available to the carrier.*"[59]

> [I]f such information is not reasonably available, the carrier does not have to modify its system to make it available.[60]

Post-cut-through digits are not available to CMRS providers because they are dialed (or entered) *after* the provider establishes a connection to another carrier; from the perspective of a CMRS provider, post-cut-through digits constitute call content. Consequently, AirTouch submits that under CALEA, carriers are not required to provide post-cut-through digits or any of the other call-identifying information the FBI seeks because this information is not "reasonably available to the carrier."[61]

---

57 (...continued)
not. Indeed, Congress made very clear that "dialing tones that may be generated by the sender that are used to signal customer premises equipment of the recipient are *not* to be treated as call-identifying information." House Report at 21 (emphasis added).

58 Post-cut-through dialing involves subscriber dialing done *after* the target's serving local carrier establishes a communications path. For example, a subscriber may dial extra digits to obtain information from his or her voice mail box or answering machine. Or, the subscriber may need to dial extra digits after dialing an 800 number to reach a long distance carrier (*e.g.*, 800-CALL-ATT), so the long distance carrier knows how to route and bill for the call. However, from the perspective of the local carrier, post-cut-through dialing constitutes call content because the dialed digits are transmitted *after* the local carrier completes call set-up in establishing a communications circuit.

59 47 U.S.C. § 1002(a)(2) (emphasis added).

60 House Report at 22.

61 In the end, the FBI wants industry to deploy new capabilities in call processing when the impact of these additional capabilities on the existing network is not known (*e.g.*, whether the performance of additional steps will impact service quality for all traffic). Consequently, AirTouch encourages the Commission to solicit additional public comment if it is inclined to grant one or more of the punch list capabilities — so the network impacts
(continued...)

Moreover, even if the Commission were to ignore the "reasonably available" standard in the statute, post-cut-through-digits cannot be provided over a data delivery channel "by cost-effective methods."[62] In fact, one vendor has advised AirTouch that the cost to develop this feature alone would, by itself, likely exceed the cost to develop all of the other punch list items.

It is noteworthy that much of the information the FBI seeks as part of a call-identifying interception will continue to be available to law enforcement.[63] As the FBI acknowledges, in the past law enforcement often received ringing/busy signals and post-cut-through dialing digits as part of a call-content interception.[64] Consequently, the issue the FBI poses is *not* whether it will receive the requested information, but rather *how* it will receive the requested information (*i.e.*, over a call data delivery channel or a call content delivery channel).

In this regard, the FBI specifically complains about the industry proposal to deliver certain call-identifying information (*e.g.*, post-cut-through digits, busy signals) over a separately leased call content channel, and it asks the Commission to require carriers to provide

---

61 (...continued)
on the public's non-intercepted traffic can be evaluated.

62 47 U.S.C. § 1006(b)(1).

63 Some of the requested capabilities are also new however, and have not been provided in the past. For example, the FBI readily acknowledges that, in the past, it did not receive "information that a particular participant was placed on hold during, or dropped from, a multi-party call." FBI Petition at 44 ¶ 77. Many of these new capabilities involve information which carriers do not record today (because there is no reason to do so). More fundamentally, these new requested capabilities are also outside the scope of CALEA. *See* House Report at 22 ("The FBI Director testified that the legislation was intended to preserve the status quo, that it was intended to provide law enforcement no more and no less access to information than it had in the past.").

64 *See, e.g.*, FBI Petition at 46 ¶ 81 ("This information historically has been available to law enforcement on call content channels.").

this information over a call data channel.[65] The basis for this complaint is difficult to understand because the FBI recently held that for some interceptions carriers must be capable of supporting up to *five* different delivery channels for a *single* interception.[66] In any event, in making its request, the FBI readily concedes that CALEA does *not* require carriers to provide this capability:

> Industry contends that [CALEA] does not mandate delivery over a call data channel of call-identifying information that is capable of being extracted from the call content channel. *We agree that a carrier could comply with its delivery obligations under [CALEA] without delivering this information in this fashion.*[67]

In making this concession, the FBI thus answers the question it poses: the Commission cannot require carriers to provide this particular capability because CALEA does not require it.[68]

It bears noting that the reason carriers do not deliver certain call-identifying information over a data delivery channel is because the information is not reasonably available to them, as explained above. CALEA therefore expressly provides that carriers are not obligated to deliver to law enforcement this information over a call data channel. Consequently, if law enforcement wants to receive post-cut-through digits, busy signals, and certain other call-identifying information, it can receive the information but it must follow the same procedure that it has utilized in the past: obtain a call content delivery channel. Spending any resources on

---

65 *See* FBI Petition at 47-49 ¶¶ 83-85; FBI Proposed Rule 64.1708(d) and (i)(1). This FBI request appears to be new, as it was not included in the FBI's original punch list.

66 *See* FBI, *Implementation of Section 104 of CALEA: Final Notice of Capacity*, 63 Fed. Reg. 12218, 12232-33 (March 12, 1998) ("*Final Capacity Notice*").

67 FBI Petition at 47 ¶ 84 (emphasis added).

68 *See, e.g.*, House Report at 22 ("The Committee intends the assistance requirements in [CALEA] to be both a floor and a ceiling.").

developing and implementing these features would be unjustifiable, given the alternatives law enforcement will continue to have to receive much of the same information.

C. Timely Delivery of Call-Identifying Information (Punch List Item 5)

CALEA obligates carriers to provide law enforcement with access to call-identifying information "before, during, or immediately after the transmission of a wire or electronic communication (or at such later time as may be acceptable to the government)."[69] The FBI asserts that the industry standard is "manifestly deficient" because it does not include specific delivery times and that, as a result, carriers could deliver the information "at a time other than 'before, during, or immediately after' the communication."[70] The FBI therefore asks the Commission to require carriers to time-stamp information within one-tenth of a second (100 milliseconds) and that, depending on the type of call-identifying information involved, carriers deliver the information to law enforcement within either three or five seconds.[71] However, in making this request, the FBI readily acknowledges that its proposed timing requirements "are not the only ones that would satisfy" CALEA.[72]

It would be inappropriate for the Commission to adopt delivery time standards. As the FBI itself acknowledges, its proposed delivery time standards are not required by CALEA and, therefore, there is a substantial question whether the Commission has the authority to adopt

---

69 47 U.S.C. § 1002(a)(2)(A).

70 FBI Petition at 51 ¶ 90.

71 *See* FBI Petition at 51-52 ¶ 92; FBI Proposed Rule § 64.1708(e).

72 FBI Petition at 52 ¶ 93.

any particular timing standard.[73] Moreover, as a practical matter, a "one-size fits all" timing standard simply will not work when applied to thousands of carriers which will use many different solutions to meet their CALEA obligations.[74] In addition, a carrier may be unable to meet any standard the Commission may publish for reasons beyond its control (*e.g.*, unanticipated traffic volumes resulting in congestion; other carriers participating in the call delay the delivery of the information to the carrier subject to the court order).

Importantly, Congress was clear in providing that CALEA "leaves it to each carrier to decide how to comply with the statute:"

> Compliance with the industry standards is voluntary, not compulsory. Carriers can adopt other solutions for compliance with the capability requirements.[75]

For the Commission to adopt rigid delivery time standards would undermine Congress' intent that industry be given flexibility in selecting cost-efficient solutions to satisfy their CALEA obligations.

It would be especially inappropriate to adopt delivery time standards at this point. As the Commission is aware, the technology necessary to implement the industry standard does not now exist. Thus, if the Commission were to adopt the FBI's proposal, it would necessarily

---

73 *See, e.g.*, House Report at 22 ("The Committee intends the assistance requirements in [CALEA] to be both a floor and a ceiling.").

74 *See* FBI Comments at 10 ¶ 18 (May 8, 1998) ("Different manufacturers and carriers have different capabilities and needs."). For example, the Commission adopted 800 access time standards for GTE and the Bell companies but declined to impose the same standards on other LECs because they could support 800 database access "in a variety of ways," with the Commission determining that most LECs required "maximum flexibility in planning their participation in a manner that best serves their needs and financial capabilities." *Provision of Access for 800 Service,* CC Docket No. 86-10, *Memorandum Opinion and Order on Further Reconsideration,* 8 FCC Rcd 1038, 1040 ¶ 14 (1993).

75 House Report at 23 and 27.